CLAIMS

1. An enciphering method comprising a step of formatting a message in clear (m) by means of a formatting function (μ), and a step of exponentiation of the result of the previous step using a public key (N, e) in accordance with the equation $c = \mu(m)^e \bmod N$, c being an enciphered message, $\mu(m)$ being the result of the formatting step, and e and N elements of the public key,

the method being characterised in that the formatting function (μ) is the PSS function.

2. A method according to claim 1, characterised in that the formatting function μ is defined by

$$\mu(m) = PSS(m) = \omega \,||\, s, \text{ with:}$$

m, the text in clear of k - k0 - k1 bits, r a random parameter of k0 bits, k, k0, k1 being parameters of the formatting function,

|| a concatenation function

$\omega = H(m \,||\, r)$

$s = G(\omega) \oplus (m \,||\, r)$

$\otimes$ a logic function XOR, and

H, G two hashing functions

3. Use of a probabilistic signature function (PSS) defined according to the standard PKCS #2 v 2.1, RSA cryptography standard as a formatting function (μ), in order to effect an enciphering method comprising a step of formatting a message in clear (m) by means of the formatting function (μ), and a step of exponentiation of the result of the previous step by means of a public key (N, e) in accordance with the equation c =

$\mu(m)^e$ mod N, c being an enciphered message, $\mu(m)$ being the result of the formatting step, and E and N elements of the public key.

4. A cryptographic system comprising:

- a step of formatting a message in clear (m) by the probabilistic signature function (PSS), and then:

- if an enciphering of the message in clear (m) is required, a step of exponentiation of the result of the formatting step by means of a first key (N, e) in accordance with the equation $c=\mu(m)^e$ mod N, c being an enciphered message, $\mu(m)$ being the result of the formatting step, and e and N elements of the first key, or

- if a signature of the message in clear (m) is required, a step of exponentiation of the result of the formatting step by means of a second key (N' d') in

accordance with the equation $s = \mu(m)^{d'} \bmod N'$, s being a signed message, $\mu(m)$ being the result of the formatting step, and d' and N' elements of the second key.

5. A system according to claim 3, in which the first key and the second key are respectively a public key of a first pair of keys and a private key of a second pair of keys.

6. A system according to claim 4, in which the first pair of keys and the second pair of keys are identical.

7. A system according to one of claims 4 to 6, of the RSA type.

8. An electronic component comprising programmed means for implementing an enciphering method according to one of claims 1 to 2, the programmed means comprising in particular a central unit and a program memory.

9. An electronic component comprising programmed means for implementing a cryptographic system according to one of claims 4 to 7, the programmed means comprising in particular a central unit and a program memory.

10. A chip card comprising an electronic

component according to claim 7 or claim 8.